FNAL
Mac OSX Desktop & Laptop Baseline

Prepared by: _____ Date: _____

System/Application Owner

Ben Segbawu

Approved by: _____ Date: _____

Computing at Fermilab

FNAL Mac OSX Workstation Baseline

1.1 Acknowledgement

This Document was originally written by Mark Kaletka and Randy Reitz for OSX 10.3 and 10.4. It has been modified for OSX 10.5.

1.2 Overview

This Security Technical Implementation Guide (STIG) provides Fermi National Accelerator Laboratory with guidance regarding the proper configuration of the Apple Mac OS X operating system security settings in accordance with Fermi National Accelerator Laboratory security requirements and guidelines. This document will focus on Apple Mac OS X version 10.5 (Leopard) as used in desktop and laptop environments. Features available in Apple Mac OS X Server are not discussed in this document.

The Fermi National Accelerator Laboratory Security Baseline configuration settings represent industry best practices for securing OS X desktop and laptop computers, based on recommendations from several sources including Red Hat, the SANS Institute, the Defense Information Security Agency (DISA), the National Security Agency (NSA), and the Center for Internet Security (CIS). The settings were reviewed and modified for compliance with the Fermi National Accelerator Laboratory operational environment.

This document presents the required (mandatory) and recommended (best practice) levels of security settings.

1.3 Purpose

The settings discussed in this STIG are intended to minimize the exposure of a Mac OS X desktop and laptop to known vulnerabilities. This document consists of both required and recommended settings which are detailed in the Baseline Checklist at the end of the document.

1.4 Scope

This document discusses the configuration of Apple hardware installed with the Mac OS X Leopard operating system. The recommendations contained herein may also apply to previous versions (e.g. Tiger) of Mac OS X.

1.5 Intended Audience

This document is intended for system administrators responsible for the security of Apple MAC OS X desktop and laptop systems at Fermi National Accelerator Laboratory. It assumes that the reader has

knowledge of the Mac OS X operating system and is familiar with common computer terminology and common administrative tasks.

2 Physical Security

Desktop and laptop systems must be physically secured to ensure that unauthorized individuals do not gain access to the systems. Security cables can be used to prevent theft. Password locked screen savers must be used to prevent unauthorized access.

2.1 System BIOS Password

Setting the firmware password is not mandatory for Mac OS X systems.

3 Secure Installation

It is recommended to start with a "clean" install from known good media, particularly if the prior configuration of the system is not well known (i.e. you "inherit" an old system, you're not sure what's on it, best practice is to wipe the disk and install clean).

Prior to placing a Mac system into production, the system administrator must ensure that the latest patches are installed. The Mac OS provides 'Software Update' in the Apple menu to install the latest patches.

Any Mac OS X patches declared "mandatory" must be installed before connecting to the Fermilab network. These patches will need to be obtained from the local Fermilab repository or from http://www.apple.com/support/downloads/ and placed on removable media for off-line installation.

3.1 Patch Management

Developing a procedure for keeping up-to-date with vendor patches is critical for the security and reliability of the system. Vendors issue operating system updates when they become aware of security vulnerabilities and other serious functionality issues. The 'Software Update' feature of Mac OS X is currently sufficient to keep the software patches current. The 'Software Update' features must be configured (via System Preferences) to check for updates a minimum of weekly and recommended daily.

Now that a Laboratory central patching service for Mac OS X is in production, systems must be configured to use the Fermilab Update Server.

3.2 Anti Virus

Anti virus software is another crucial component for system security. Although Mac OS X is relatively secure, viruses and other types of malware do exist for Mac OS X and anti virus client software must be installed and enabled and must conform to the anti virus baseline configuration.

Fermilab has a site license for an antivirus client for Mac. This is the required AV client software. For users that report incompatibility with this client, the open-source ClamX AV client must be installed and maintained by the local sysadmin, and an exemption from the Antivirus Baseline must be maintained.

3.3 Configuration Management

Fermilab uses SMS as its configuration management tool. This allows us to respond to queries from DOE when required. The QMX SMS Client for Mac must be installed.

4 System Preferences

4.1 Appearances

This section is a user defined section.

4.2 Desktop and Screen Saver

Desktop is a user Defined Section.

Under Screen Saver Tab

- Set Screen Saver to Start at 15 Minutes

4.3 Dock

This section is a user defined section.

4.4 Expose and Spaces

This section is a user defined section.

4.5 International

This section is a user defined section.

4.6 Security

Under the General Tab

- Select Require Password to Wake this Computer from Sleep or Screen Saver
- Select Disable Automatic Login
- Select Require Password to Unlock each System Preference Pane
- Uncheck Log out after xx minutes of inactivity
- Select Use secure Virtual Memory
- If available Disable Remote Control Receiver

Under the FileVault Tab

- Do not set Master password. If you do and you loose it the Computing Division cannot help you.
- Do not turn on File Vault. (This is still being looked at by Computing Division) If you Turn on File Vault and forget the master password you have lost access to your system information.

Under the Firewall Tab

- Select Allow only Essential Services
- Click on the advanced tab
    - Select Enable Firewall Logging
    - Uncheck Enable Stealth Mode

4.7 Spotlight

This section is a user defined section.

(If you have network shares you can add them here)

4.8 BlueTooth

- Uncheck On
- Uncheck Discoverable
- Check Show Bluetooth Status in the menu bar

Under the Advanced Tab

- Uncheck Serial Port the Devices use to connect to This Computer
- Uncheck open Bluetooth Setup Assistant at Startup when no input device is present

4.9 CDs and DVDs

This section is a user defined section. Below are common setting suggestions.

- When you insert a blank CD: Ask what to Do
- When you insert a blank DVD : Ask what to Do
- When you Insert a music CD: Open Itunes
- When you insert a Picture CD: Open Iphoto
- When you insert a Video DVD: Open DVD Player

4.10 Displays

This section is a user defined section.

4.11 Energy Saver

Note: You may not have all the settings depending upon the model of your hardware.

Under the Battery Tab

- Put computer to Sleep when it is inactive for one hour
- Put Display to Sleep when the Computer is inactive for 30 Minutes
- Put the hard disks to Sleep when Possible
- Automatically reduce the brightness of the display before sleep

Under the Power Adapter Tab

- Put computer to Sleep when it is inactive to Never
- Uncheck the Wake for Ethernet network Administrator Access
- Check Restart Automatically after a power Failure
- Under the Schedule option do not schedule automatic shutdown

4.12 Keyboard & Mouse

This section is a user defined section. Below are common setting suggestions.

Under Mouse Tab (Mouse has to be connected first)

- The Scroll Button – Select Dashboard
- The Left Mouse click – Select Primary Button
- The Right Mouse Click – Select Secondary Button
- The Double side click – Select off
- Scrolling – Select Vertical and Horizontal
- Tracking – Leave default Setting
- Scrolling - Leave Default Settings
- Double Click – Leave Default Settings
- Zoom using Scroll ball while holding Control – Leave Default

  Under options

  - When Zoomed in The Screen Image moves Select Continuously with Pointer
  - Select Smooth Images (Press alt cmd backslash to turn smoothing on or off)

Under Bluetooth Tab

- Make sure Show Bluetooth Status in Menu Bar is checked
- Uncheck Bluetooth Devices to wake this computer (unless you have a Bluetooth mouse or keyboard otherwise you will not be able to log onto your computer)

4.13 Print & Fax

- Add necessary printers
- Default printer - last Printer Used
- Default Paper Size in Page Setup – US Letter

4.14 Sound

This section is a user defined section.

4.15 DotMac or MobileMe

DotMac or MobileMe should not be configured at Fermilab.

4.16 Network

Select Location: 'edit locations…'

Click the + to add a new location and rename from 'Untitled' to 'Fermilab'

Select Location: 'Fermilab'

From the * dropdown list under the list of interfaces, select 'Set Service Order…'

Drag to arrange to this order (ignore any list items that are not configured for your system)

- Ethernet
- AirPort
- Firewire
- USB *
- Bluetooth

If using Ethernet, select Ethernet on left, and then click the 'Advanced…' button

Under the TCP/IP Tab

- If using DHCP, fill in 'DHCP Client ID:' field with the MISCOMP registered SYSTEM NAME for the device
- Set Configure IPv6 to: 'Off'

Under the DNS Tab:

- Add fnal.gov to the search domains

Under the Wins Tab:

- If not using DHCP, click the + to add 131.225.9.1 & 131.225.110.15 to the WINS Servers list
- Fill in the 'NetBIOS Name:' field with the MISCOMP registered SYSTEM NAME for the device

Under the AppleTalk Tab

- Disable Make Apple Talk Active

Under 802.1X Tab

- Delete all profiles

Under Proxies Tab

- No Proxies

Under the Ethernet Tab

- Use Configure Automatically

If using AirPort, select AirPort on left.

For Laptops, select the 'Ask to join new networks' box. (Otherwise the user is likely to switch to 'Location: Automatic' when off-site, and never switch back when on-site.)

Click the 'Advanced…' button.

Under the AirPort tab:

- Click the + and then 'Show Networks' and select 'fgz', then click 'Add'
- Uncheck 'Remember any network this computer has joined'

Under the TCP/IP Tab:

- If using DHCP, fill in 'DHCP Client ID:' field with the MISCOMP registered SYSTEM NAME for the device
- Set Configure IPv6 to: 'Off'

Under the DNS Tab:

- Add fnal.gov to the search domains

Under the Wins Tab:

- If not using DHCP, click the + to add 131.225.9.1 & 131.225.110.15 to the WINS Servers list
- Fill in the 'NetBIOS Name:' field with the MISCOMP registered SYSTEM NAME for the device

Under the AppleTalk Tab

- Disable Make Apple Talk Active

Under 802.1X Tab

- Delete all profiles

Under Proxies Tab

- No Proxies

Under the Ethernet Tab

- Use Configure Automatically

4.17 QuickTime

Under the Register Tab

- Add Registration for Quick Time Pro (if you purchased QuickTime PRO)
- Under the Browser Tab
- Play Movies Automatically
- Uncheck Save Movies in Disk Cache
- Under the Update Tab
    - Install 3rd Party QuickTime Software as needed
- Under the Streaming Tab
    - Streaming Speed – set to Automatic
    - Enable instant-On
- Under the advanced Tab
    - Use Default Settings
- Under MIME Settings – Use Default Settings
- Under Media Keys – Use Default Settings

4.18 Sharing

Computer Name: fill in this field with the MISCOMP registered SYSTEM NAME for the device

Remote Management - Set to Off (unless firewall restricted to localhost)

Screen Sharing - Set to Off (unless firewall restricted to localhost)

File Sharing - Set to Off (unless firewall restricted to localhost or configured to SAMBA baseline)

Printer Sharing - Set to Off

Web Sharing - Set to Off

Remote Login - Set to Off (unless sshd is kerberized)

Remote Management - Set to Off (unless firewall restricted to localhost)

Remote Apple Events - Set to Off

Xgrid Sharing - Set to Off

Internet Sharing - Set to Off

Bluetooth Sharing - Set to Off

4.19 Accounts

Two accounts minimum must be created, with different passwords.

For the regular account Short name must match Kerberos User Name (example bens)

For the Admin Account short name must be the regular short name-admin (example bens-admin)

Under Login Options

- Automatic Login Set to Disabled
- Display Login Windows as Name and Password
- Select Show Restart, Sleep and Shutdown buttons
- Uncheck Show Input menu in login window
- Uncheck Show Password Hints
- Uncheck VoiceOver at login Window
- Disable Fast user Switching

Guest Account should be disabled and disallow guest to connect to shared folders

Users should not login using the administrative login except when required for administration of the system.

4.20 Date & Time

Under Date & Time Tab

Set Date & Time Automatically Use Apple Americas/U.S. (time.apple.com)

Under the Time Zone Tab

- Time Zone - Select CST
- Closest City – Chicago

Under Clock Tab

- Select Show Date and Time in Menu Bar
- Select View as Digital
- Uncheck Display the time with seconds
- Select Show AM / PM
- Select Show the day of the week
- Uncheck Flash the time separators
- Uncheck use a 24-hour clock
- Uncheck Announce the time on the hour

4.21 Parental Control

- Use as necessary

.

4.22 Software update

- Select Check for Updates Daily
- Select Download Important Updates Automatically

4.23 Speech

This section is a user defined section.

4.24 Startup Disk

Do not change anything here. If you change the startup disk your system may not boot.

4.25 Time Machine

If you have a secondary internal or external usb / firewire disk that you can dedicate to time machine then you can configure Time Machine.

Time Machine keeps hourly backups for the past 24 hours, daily backups for the past month and weekly backups until your back up disk is full.

It is recommended you only back up your Documents and Desktop.

Please note that your keytab files and PKI private keys must be backed up on separate backup media and securely stored

4.26 Universal Access

This section is a user defined section.

5 Network Services

The system administrator must determine which users (if any) will need to remotely access the system. Services such as telnet, FTP and sshd should not be turned on unless a need to accept incoming connections is demonstrated. The Fermilab Computer Security policy requires that these 'login' type services be configured to only accept Kerberos authentication.

Mac OS X offers many services. The system administrator must not enable services on the premise that one day these services might be needed. A vulnerable service increases the system's risk of compromise. The system administrator will disable all services and then re-enable only those services required by a given system's needs.

5.1 Secure Shell (SSH)

OpenSSH is a popular free distribution of the SSH protocols, which allow secure encrypted network logins and file transfers. Mac OS X provides a current version of OpenSSH as part of the OS installation. The OpenSSH client can be used to connect to remote hosts. The OpenSSH server can be used to accept incoming connections. The OpenSSH server should only be enabled (via System Preferences – Sharing – Remote Login) if the user can perform the required configuration for accepting only Kerberos authenticated

incoming connections. Refer to the Fermilab Strong Authentication Manual for procedures (http://www.fnal/gov/docs/strongauth/macadmin.html).

6 Boot Services

6.1 Boot Daemons

When Mac OS X boots, any commands in /etc/rc.local will be executed. Check the contents of this file if it exists. Also, unless safe boot has been requested (hold down the shift key after power on and hearing the startup tone), the daemons listed in /Library/LaunchDaemons will be run.

Mac OS X Leopard will honor the Tiger startup items found in /System/Library/StartupItems and in /Library/StartupItems. Check the contents of these directories.

6.2 "Login Items" for Accounts

Each configured account can request items be run at login. Use the GUI found in System Preferences – Accounts – Login Items to view these items for each user.

6.3 SAMBA/CIFS/AFP/File Sharing

Mac OS X includes the popular Open Source Samba server for providing file and print services. This allows a Mac OS X system to act as a file or print server on a network, and even act as a Domain Controller (authentication server) to older Windows operating systems. This service (called 'File Sharing') should be disabled. If enabled, it must be firewall restricted to localhost (for use via kerberized ssh tunnel) or conform to the Samba baseline configuration.

Note that "File Sharing" provides file sharing *from* a Mac to Windows. It *is not* needed for Mac's to access files on Windows shares.

6.4 Printers

Printer sharing enables printing from remote hosts to a locally connected printer. The recommended configuration is to disable printer sharing.

6.5 Web Server

It is recommended that Web services be disabled on Mac OS X systems. Web servers that need outside fnal.gov access need to request an exemption and conform to the baseline configuration for web servers.

6.6 Instant Messaging (IM)

The onsite jabber.fnal.gov server should be used. iChat or the AdiumX client can be used as a client. Use of AOL is not suggested as it is not encrypted and allows for possible sensitive data passing though offsite servers. Remote IM passwords must never be the same as used for any Fermilab service.

7 File/Directory Permissions

7.1 Disk Utility

This application can be used to check and repair file/directory permissions. This will ensure that sensitive system files and utilities are appropriately protected. It is recommended that the 'First Aid – Verify Disk Permissions' option be selected periodically.

8 Logging

8.1 Increase syslog Logging Levels

Increase the level of authentication logging by editing the file /etc/syslog.conf to change the line:

```
auth.info;authpriv.*;remoteauth.crit            /var/log/secure.log
```

to:

```
auth.info;authpriv.*;remoteauth.err             /var/log/secure.log
```

and, add the line:

```
authpriv.*;remoteauth.err;auth.err              @clogger.fnal.gov
```

Note that all whitespace in this file should be TABs not spaces.

This sends logs to a remote server (clogger.fnal.gov) in addition to keeping logs locally. If the local system is compromised, the logs will still be available for analysis on the remote system.

9 System Access and Authorization

9.1 r-commands

Non-kerberized r-commands are NOT allowed unless an approved exemption exists.

Used in conjunction with the BSD-style "r-commands" (`rlogin`, `rsh`, `rcp`), `.rhosts` files implement a weak form of authentication based on the network address or host name of the remote computer (which can be spoofed by a potential attacker to exploit the local system). Disabling `.rhosts` support helps prevent users from subverting the system's normal access control mechanisms.

If .rhosts support is required for some reason and an approved exemption exists, some basic precautions should be taken when creating and managing .rhosts files. Never use the "+" wildcard character in .rhosts files. In fact, .rhosts entries should always specify a specific trusted host name along with the user name of the trusted account on that system (e.g., "trustedhost alice" and not just "trustedhost"). Avoid establishing trust relationships with systems outside of the organization's security perimeter and/or systems not controlled by the local administrative staff. Firewalls and other network security elements should actually block rlogin/rsh/rcp access from external hosts. Finally, make sure that .rhosts files are only readable by the owner of the file (i.e., these files should be mode `600`).

9.2 FTP

Only kerberized ftp is allowed unless an approved exemption exists or the ftp access is anonymous read-only. Normally ftp should be disabled.

10 X Server

An X server is included with Mac OS X in the developer tools distributed with the OS. X11 for Mac OS X offers a complete X Window System implementation for running X11-based applications on Mac OS X. The X server installed with the base OS is configured to not listen by default on port 6000/tcp for messages from remote clients running on other systems. This prevents authorized remote X clients from displaying windows on the local system as well. However, the forwarding of X events via SSH will still happen normally. This is the preferred and more secure method transmitting results from remote X clients in any event.

11 Use of Administrator Privileges

11.1 Use of Privileged & Non-Privileged Accounts

A default installation of Mac OS X creates the first user account with administrator privileges. A non-privileged account must be created after installation via System Preferences – Accounts, and this account must be used for normal work. The privileged account should only be used when the privileges are required. Mac OS X is actually quite good at allowing software installations, etc. from a non-privileged account and prompting for a privileged account when necessary. (Of course, the user must know the privileged account password.)

The initial privileged account created at installation should be of a form similar to "name-admin" (where name is the same as the user's Kerberos name) and a non-privileged "name" account must be added after installation and used for normal work.

11.2 su/sudo

OS X provides the 'sudo' command which allows an administrative user to elevate their privileges on the command line interface to perform activities that would require 'root' access on a typical unix system. Regular user account cannot use the 'sudo' command. Regular users may first use the 'su' command to switch their command line interface to the administrative user, and then subsequently 'sudo' to perform command line administration. This requires the regular user to know the administrative user login name and password.

11.3 Root Account

The default OS X installation does not enable the root account. It is required that the root account not be enabled.

The status of the root account can be checked in Applications->Utilities->Directory Utility by selecting the 'Edit' drop down menu from the top of the screen and assuring that it has the option 'Enable Root User', which demonstrates that the user is not currently enabled.

11.4 Access to System Preferences

To restrict access to the sensitive System Preferences panes, ensure that System Preferences – Security "Require password to unlock each secure system preference" is checked.

Author: Ben Segbawu, Waylon Meadows, Kirk Skaar, Tim Zingleman

Baseline

12 User Accounts

12.1 Passwords

Local passwords must conform to Fermilab password policy and recommendations. Local user and privileged accounts must have strong passwords, 10 characters using three of four classes (upper, lower, numeric, special.) See http://computing.fnal.gov/docs/strongauth/princ_pw.html#45589 for additional password guidelines.

Fermilab Kerberos passwords *must not* be used for local passwords.

Mac OS X provides a Password Assistant which can be accessed by clicking the key button on any password choice dialog box. The Password Assistant will provide additional guidance in choosing strong passwords by visually indicating the "quality" of password entered.

12.2 GUI Login

Automatic login must be disabled. Automatic login is controlled via System Preferences – Security. In addition, select the check box to require password to wake the computer from sleep or screensaver and disable the remote control IR receiver.

In System Preferences – Accounts, it is also required to set "Display Login Window as:" to "Name and password".

Disable password hints by un-checking Show Password hints in the Accounts Preference pane.

12.3 Block System Accounts

Accounts that are not being used by regular users should be locked. Such accounts may include: adm, games, lp, shutdown, news, operator, daemon, and nobody. Not only should the password field for the account be set to an invalid string, but also the shell field in the password file should contain an invalid shell. `/dev/null` or `/dev/false` are good choices because they are not valid login shells, and should an attacker attempt to replace either with a copy of a valid shell the system will not operate properly. Accounts with passwords set can be quickly found using the command…

```
dscl localhost –list /Local/Default/Users Password
```

Accounts with a single '*' do not have a password set. Check that the accounts with passwords are needed.

The shell assigned to each account can be displayed using the command:

```
dscl localhost –list /Local/Default/Users UserShell
```

UID 0 accounts should not exist, other than root. UID 0 accounts can be identified by running the command:

```
dscl localhost –search /Local/Default/Users uid 0
```

12.4 User dot Files

Group or world-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges. User dot files such as ".profile" and ".cshrc" must have "write" access removed from users who are members of the group and from all other users. The systems administrator can use the command **chmod go-w *file***. Making global modifications to user home directories without alerting your user community can result in unexpected outages and unhappy users.

12.5 Access Control Lists

Mac OS X supports fine-grained file ACL's. Their use is optional and a full description is outside the scope of this document.

12.6 Keychain Access

Keychains should be set to lock after a period of inactivity and when the system sleeps. In Applications – Utilities – Keychain Access – Preferences, under the First Aid tab, select “Synchronize login keychain password with account”, “Set login keychain as default”, and uncheck “Keep login keychain unlocked”. This must be done for EACH user.

13 Warning Banners

13.1 Physical Access Services

The contents of the `/etc/issue.net` file are displayed prior to the login prompt on the system's console.

The login banner must be added to the gui login by executing (from an administrator account):

```
open /Library/Preferences
```

Right click (or hold down the control key and click) on com.apple.loginwindow.plist and select ‘Get Info’. Unlock the ‘Sharing and Permissions’ and change ‘admin’ to ‘Read & Write’. Double Click on filename to open it.

In the the GUI Property List editor, select and expand "Root" and add a "New Child" "LoginwindowText" of class "String". Paste the approved Fermilab "NOTICE TO USERS" text into the value of this child. This text can be obtained from http://security.fnal.gov/Banners/. Save the Changes and exit.

Right click (or hold down the control key and click) on com.apple.loginwindow.plist and select ‘Get Info’. Unlock the ‘Sharing and Permissions’ and change ‘admin’ back to ‘Read only’.

Systems must also display the Fermilab "NOTICE TO USERS" stickers (available from CD) prominently on or near the monitor.

Note. You will need to have Property List editor app from Developer Tools and change permissions to be able to modify the plist.

13.2 Kerberized Telnet Banner

If a kerberized telnet service is permitted to run, then a telnet warning banner containing the Fermilab "NOTICE TO USERS" text must appear when a user connects to this service.

Setting this banner has the side effect of hiding the default telnet banner, which advertises the version of Mac OS X running on the system.

Add the text of the banner to the file /etc/issue.net, or whichever file your kerberized telnet uses.

13.3 Kerberized FTP Banner

If a Kerberized FTP service is permitted to run, then an FTP warning banner containing the Fermilab "NOTICE TO USERS" text must appear when a user connects to the service.

Baseline

Enable the FTP banner by either including the banner text in /etc/ftpwelcome or soft link this file to /etc/issue.net.

13.4 Kerberized sshd Banner

If a Kerberized sshd service is permitted to run, then an sshd warning banner containing the Fermilab "NOTICE TO USERS" text must appear when a user connects to the service.

Edit /etc/sshd_config to comment out any existing banner and add the line "Banner /etc/issue.net".

14 Backup & Recovery

System backups are critical for the restoration of files should hardware failures, software failures, or accidental erasures occur. Backups are a basic requirement for any contingency/disaster recovery plan. User data should be backed up appropriately or stored on a server. The usual recovery plan for non-server systems is to wipe and reinstall the operating system and applications.

14.1 Time Machine

The possibility of limited network synchronized backups is currently being investigated.

15 References

This section provides a list of references used in developing this document.

The SANS Institute
Securing Mac OS X Desktop
http://www.sans.org/score/macosxchecklist.php

The Center for Internet Security
http://www.cisecurity.org
http://www.cisecurity.org/bench_osx.html

Defense Information Systems Agency (DISA)
UNIX Security Technical Implementation Guide
Version 4 Release 4
September 15, 2003
http://www.disa.mil

NIST Special Publication 800-40
Procedures for Handling Security Patches
http://csrc.nist.gov/publications/nistpubs/800-40/sp800-40.pdf

DOE G 205.3-1, Password Guide.
https://www.directives.doe.gov/pdfs/doe/doetext/restrict/neword/205/g2053-1.pdf

DOE N 205.3, Password Generation, Protection and Use
https://www.directives.doe.gov/pdfs/doe/doetext/restrict/neword/205/n2053.pdf

	Description	Required	Recommended
2	**Physical Security**	Physically secured (locked down) to prevent theft or unauthorized access.	
2	**Physical Security**	Enable locking screen saver.	
2.1	**System BIOS Password**		No.
3	**Secure Installation**		Install "clean" from known good media. See Section 3 for more details.
3	**Secure Installation**	Install Fermi mandatory patches.	
3	**Secure Installation**	Install Apple recommended patches.	
3.1	**Patch Management**	Enable automatic "Software Update", check weekly for updates.	Enable automatic "Software Update", check daily for updates.
3.1	**Patch Management**	Use Apple Software Update Service.	Use Laboratory Apple Software Update central patching service.
3.2	**Anti Virus**	Install & run anti virus client software conforming to anti virus baseline configuration.	Install & Run Fermi Site Anti virus client software conforming to anti virus baseline configuration.
3.3	**Configuration Management**	Install QMX SMS.	
4.2	**Desktop and Screen Saver**	Screen Saver set to start at 15 minutes of inactivity.	
4.6	**Security – Under the General Tab**	Require Password to Wake this computer from Sleep or Screen saver. Disable Automatic Login. Require Password to Unlock each system Preference Pane. Use Secure Virtual Memory.	Uncheck Log out after XX minutes of inactivity. If available Disable Remote Control Receiver.
4.6	**Security – Under the FileVault Tab**		Do Not Set Master Password. Do Not Turn on File Vault.
4.6	**Security – Under the Firewall Tab**	Allow Access for minimum required specific services and applications. Use IPFW if Application Firewall must be set to	Allow Only Essential Services. Enable Firewall Logging.

			Baseline
		Allow all incoming connections.	Do not enable Stealth Mode.
4.8	**Bluetooth**	Show Bluetooth in menu bar.	Uncheck On. Uncheck Discoverable.
4.8	**BlueTooth – under Advanced Tab**		Uncheck Serial Port the Devices use to connect to this computer. Uncheck open Bluetooth Setup Assistant at startup.
4.11	**Energy Saver – Under the Battery Tab**		Put computer to sleep when it is inactive for one hour. Put Display to sleep when Computer is inactive for 30 minutes. Put the hard disks to sleep when possible. Automatically reduce the brightness of the display before sleep.
4.11	**Energy Saver – Under the Power Adapter Tab**	Put computer to sleep when it is inactive to Never. Restart Automatically after a Power Failure.	Uncheck wake for Ethernet Network Administrator Access.
4.15	**Dot Mac or Mobile Me**	Do Not Configure.	
4.16	**Network**	Configure IPV6 to Off. Set System name to MISCOMP Registered Name. Disable Apple Talk. Fill in NetBIOS Name with MISCOMP Registered Name. If using DHCP set DHCP Client ID to MISCOMP Registered Name.	See Section 4.16.
4.18	**Sharing**	Fill in Computer Name with MISCOMP Registered Name. Configure everything except Printer & Web sharing to Off unless you follow exemptions stated in Section 4.18.	Printer Sharing and Web Sharing should be configured as Off.
4.19	**Accounts**	Minimum of Two (2) Accounts Created. One Regular and One Administrative. Different passwords. Short Name must match Kerberos	Select Show Restart, Sleep and Shutdown Buttons. Uncheck Input Menu in Login Window.

			Baseline
		User Name. Guest Account Should be Disabled. Guest connection to Shared folders needs to be disallowed. Automatic Login disabled. Display Login Windows as Name and Password. Uncheck Show Password Hints.	Uncheck VoiceOver at Login Window. Disable Fast User Switching.
4.20	**Date and Time**	Set Date and Time to Automatically Use Apple Americas/US (time.apple.com). Time Zone – Select CST. Closest City – Chicago.	See Section 4.20 for Recommended Options.
4.21	**Parental Control**		As needed.
4.22	**Software Update**	Check for Updates Weekly.	Check for Updates Daily. Download Important Updates Automatically.
4.25	**Time Machine**	keytab files and PKI private keys must be backed up on separate backup media and securely stored	Use Secondary Internal or External Disk.
5	**Network Services**	Disable all un-used services.	
5	**Network Services**	Kerberos authentication used for any "login" services enabled (ssh, telnet, ftp).	Disable all that appear in System Preferences – Sharing.
5.1	**SSH**	Configured for Kerberos authentication only.	Disabled.
6.1	**Boot Daemons**	Disable all un-used services.	Check for items in /etc/rc.local, /Library/LaunchDaemons, /System/Library/StartupItems, /Library/StartupItems, /etc/hostconfig.
6.2	**"Login Items" for Accounts**	Disable all un-used items.	Check login items for accounts in System Preferences – Accounts – Login Items.
6.3	**File Sharing**	If enabled, conform to Samba baseline configuration.	Disabled.
6.4	**Printer Sharing**		Disabled.
6.5	**Web Server**	If enabled, conform to web server	Disabled.

			Baseline
		baseline. Exemption needed for off-site access.	
6.6	**IM**		Use iChat or AdiumX with jabber.fnal.gov server.
7.1	**Disk Utility**		Periodically verify disk permissions.
8.1	**Increase syslog Logging Levels**	Increase logging and send logs to clogger.fnal.gov.	
9.1	**r-commands**	If enabled, use only Kerberos authentication, or have exemption & use precautions with .rhosts files.	Disable.
9.2	**FTP**	Use only Kerberos authentication or correctly configured anonymous FTP.	Disable.
10	**X Server**		Disable remote access and tunnel X connections over ssh.
11.1	**Use of Privileged & Non-Privileged Accounts**	Create separate non-privileged user account for "normal" work. Only use privileged administrator account when necessary.	
11.2	**su/sudo**		su followed by sudo may be used to perform privileged command line tasks from non-administrator accounts.
11.3	**Root Account**	Disabled.	
11.4	**System Preferences**	"Require password to unlock each secure system preference" in System Preferences – Security.	
12.1	**Passwords**	Use strong local passwords – 10 characters with four of character classes (upper, lower, numeric, special) that conform to Fermilab guidelines & policies.	
12.2	**GUI Login**	Disable automatic login and password hints.	Disable or lock IR remote.
12.2	**GUI Login**	Set "Display Login Window as: Name and password".	
12.3	**Block System Accounts**	Lock any system accounts not used regularly. Check for UID 0 accounts other than root.	Removed UID 0 accounts other than root.
12.4	**User dot Files**	Remove group & other write permissions from user files such as .profile, .cshrc, etc.	

			Baseline
12.5	**Access Control Lists**		Use ACL's if knowledgeable for finer-grained file access controls.
12.6	**Keychain Access**	Lock the keychain after a period of inactivity or when the system sleeps	
12.6	**Keychain Access**	Ensure "Show Password" is unchecked in keychain attributes. Synchronize Login Keychain password with Account. Set Login Keychain as Default. Uncheck Keep login Keychain unlocked.	
13.1	**Physical Access Services**	Configure warning banners in /etc/issue.net and the GUI login window.	
13.1	**Physical Access Services**	Apply warning banner sticker.	
13.2	**Telnet Banner**	Configure warning banner in /etc/issue.net or other file if telnet is enabled.	
13.3	**FTP Banner**	Configure warning banner in /etc/ftpwelcome or soft link to /etc/issue.net if FTP is enabled.	
13.4	**SSHD Banner**	Configure warning banner by editing /etc/sshd_config to point to /etc/issue.net if SSHD is enabled.	
14	**Backup & Recovery**	Ensure all user data is appropriately backed up.	
14.1	**Time Machine**		Use Secondary External or Internal Disk.